DNS流量异常的检测方法和系统

文献类型：专利

作者 李晓东；金键；林成虎；尉迟学彪

发表日期 2012-11-15

专利号 CN103001825A

权利人 中国科学院计算机网络信息中心

中文摘要 本发明提供一种DNS流量异常的检测方法和系统，对待处理的DNS流量数据提取相应的特征值，并对每个特征赋予不同的权重，通过W-Kmeans算法和增设的欧氏距离阈值Dthreshold检测在训练集中标记过的异常类簇，并可以发现新的未知特征的异常。本发明的算法收敛速度快，运算量小，新的待检测样本只需与处理好的训练聚类中心进行比较，无需与大量的原始训练数据进行计算部署成本低，并具有较强的泛化能力，特别适合部署在大型DNS服务器上，能够快速有效地发现DNS流量的异常。

公开日期 2013-03-27

申请日期 2012-11-15

专利申请号 201210461766.0

专利代理 北京君尚知识产权代理事务所(普通合伙) 11200